Generation and distribution procedure for personal identification numbers

Patent Number: DE19507044
Publication date: 1996-09-05
Inventor(s): MOOS RAINER (DE); KOWALSKI BERND (DE); METTKEN WERNER (DE)
Applicant(s):: DEUTSCHE TELEKOM AG (DE)
Requested Patent: ☐ DE19507044
Application Number: DE19951007044 19950301
Priority Number(s): DE19951007044 19950301
IPC Classification: G06K19/073 ; G07C11/00
EC Classification: G07F7/10
Equivalents:

Abstract

The personal identification number (pin) generation and distribution procedure involves the initial setting of a personalised security module, esp. a chip card, to a standardised pin number, designated by O-PIN. This does not allow access to any of the normal functions of the card. The O-PIN can only be used to change the pin number to the initial pin number chosen by that user. Once the OPIN has been used once to set the user's chosen pin number, it can not then be re-used. The user can check whether the card has been previously used by attempting to enter the O-PIN.

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 195 07 044 A1**

(51) Int. Cl.[6]:
G 06 K 19/073
G 07 C 11/00

(21) Aktenzeichen: 195 07 044.5
(22) Anmeldetag: 1. 3. 95
(43) Offenlegungstag: 5. 9. 96

DE 195 07 044 A1

(71) Anmelder:
Deutsche Telekom AG, 53113 Bonn, DE

(72) Erfinder:
Mettken, Werner, 59969 Hallenberg, DE; Moos, Rainer, 57080 Siegen, DE; Kowalski, Bernd, 57072 Siegen, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht zu ziehende Druckschriften:

DE	31 22 534 C1
DE	31 03 514 C2
DE	39 27 270 A1
DE	38 09 170 A1
DE	35 23 237 A1
US	48 39 506
US	47 10 613

(54) Verfahren zur Erzeugung und Verteilung persönlicher Identifikations-Nummern (PIN)

(57) Eine sichere Zusendung bzw. Übergabe des PIN-Briefes ist mit hohem Aufwand verbunden und auch dabei ist das Verlust- und Mißbrauchsrisiko nicht vollständig vermeidbar. Bei dem neuen Verfahren werden die personalisierten Sicherheitsmodule, insbesondere Chipkarten zunächst auf eine einheitliche PIN, nachfolgend als 0-PIN bezeichnet, eingestellt, mit der alle Benutzerfunktionen gesperrt sind. Erst nach der Zuordnung von Sicherheitsmodul und Benutzer-PIN wird zuerst die 0-PIN eingegeben und danach eine Änderung der 0-PIN in die Benutzer-PIN vorgenommen.
Das Verfahren ist unbeschränkt bei allen Modulen, die in Verbindung mit PIN benutzt werden sollen, anwendbar.

DE 195 07 044 A1

Beschreibung

Die Erfindung bezieht sich auf ein Verfahren zur Erzeugung und Verteilung persönlicher Identifikations-Nummern (PIN). Ein solches Verfahren besteht im Zusammenhang mit der Ausgabe personalisierter Sicherheitsmodule, z. B. Chipkarten, darin, daß zeitlich bzw. örtlich getrennt ein sogenannter PIN-Brief zugestellt wird.

Der PIN-Brief enthält die persönliche Identifikations-Nummer, mit der sich der Benutzer gegenüber der Karte als ordnungsgemäßer Besitzer ausweist.

Eine sichere Zusendung bzw. Übergabe des PIN-Briefes ist mit hohem Aufwand verbunden und auch dabei ist das Verlust- und Mißbrauchsrisiko nicht vollständig vermeidbar. In solchen Fällen ist eine kostentreibende Neuausstellung der Karten unvermeidlich.

Der Benutzer kann außerdem nur anhand des unversehrten PIN-Briefes feststellen, ob seine Karte auf dem Wege zwischen Personalisierung und Zustellung nicht schon zu seinem Schaden mißbraucht wurde. Die Unversehrtheit des PIN-Briefes beruht daher lediglich auf den relativ schwachen (das heißt wenig sicheren) bei einem PIN-Brief anwendbaren Methoden, wie z. B. Klebetechniken und Aufdruckverfahren.

Ziel der Erfindung ist die Vermeidung dieser Nachteile der bekannten Verfahrensweise und die Ermöglichung einer echten Kontrolle für den Benutzer, daß weder seine Karte noch seine Benutzer-PIN bereits benutzt wurden.

Die Lösung dieser Aufgabe erfolgt mit der im Kennzeichen des Patentanspruchs 1 dargelegten Verfahrensweise.

Die Vorteile und Funktionsweise werden im nachfolgenden Ausführungsbeispiel näher erläutert.

Die personalisierten Sicherheitsmodule, insbesondere Chipkarten werden zunächst auf eine einheitliche PIN, (z. B. "0000"), deshalb nachfolgend als 0-PIN bezeichnet, eingestellt. Mit dieser 0-PIN ist jedoch kein Zugriff auf die eigentlichen Benutzerfunktionen der Karte möglich; die Karte ist also für alle Benutzerfunktionen gesperrt.

Die 0-PIN kann nur zur Änderung dieser 0-PIN eingegeben und verwendet werden, um diese mit Hilfe des Betriebssystems in die erste gültige Benutzer-PIN zu verändern. Danach kann die Benutzer-PIN wie üblich verwendet werden. Auch ein weiteres Ändern der Benutzer-PIN funktioniert dann so, wie von den herkömmlichen Verfahren bekannt.

Nachdem die 0-PIN einmal für die beschriebene Änderung in die initiale/erste gültige Benutzer-PIN verwendet wurde, ist eine wiederholte Benutzung nicht möglich. Da die 0-PIN nicht reproduzierbar ist, und der Sicherheitsmodul erst mit der Benutzer-PIN verwendbar ist, kann der Benutzer durch initiale Eingabe der 0-PIN feststellen, ob sein Modul schon einmal benutzt wurde oder noch in seinem Urzustand ist. Diese Sicherheit beruht auf der sicheren Umgebung des Chipkartenprozessors, statt auf den wenig sicheren Druck- und Klebeverfahren.

Die personalisierten Sicherheitsmodule und Chipkarten werden dem Benutzer wie üblich zugestellt. Die Zusendung eines PIN-Briefes kann entfallen.

Das Betriebssystem des Sicherheitsmoduls, z. B. der Chipkarte, stellt sicher, daß

- die 0-PIN pro Karte nur einmal verwendet wird und daß
- die 0-PIN nur zur initialen Änderung in eine Benutzer-PIN verwendet werden kann.

Patentanspruch

Verfahren zur Erzeugung und Verteilung persönlicher Identifikations-Nummern (PIN), **dadurch gekennzeichnet,** daß die personalisierten Sicherheitsmodule, insbesondere Chipkarten zunächst auf eine einheitliche PIN, nachfolgend als 0-PIN bezeichnet, eingestellt werden, mit der alle Benutzerfunktionen gesperrt sind und die unreproduzierbar ist, und daß erst nach der Zuordnung von Sicherheitsmodul und Benutzer-PIN zuerst die 0-PIN eingegeben und danach eine Änderung der 0-PIN in die Benutzer-PIN vorgenommen wird.